# Organisations & Data Management

# Protecting valuable data, p 57

1. **Why is it important that stored data is kept secure?**

It is important that data is kept protected so that it always produces the most accurate information possible. A database may hold confidential data that must be kept private from anyone except the authorised users. It is also important as it gives a competitive advantage, it doesn’t ruin the businesses reputation, maintains public confidence and reduces the risk of having damage or loss of data which may be vital to the functioning of the organisation.

1. **What are the 2 types of controls that can protect data**?

Two types of control that can protect data is physical and software

# Measures to protect data:

**Physical equipment controls include zoned security strategies, barrier techniques and biometrics.**

**A What is meant by biometrics and what is its advantage as a means of protecting data?**

1. **Backing up**
   1. **What are the 3 types of backing up?**

The three types of backing up are full, incremental and differential.

* 1. **List some backup options?**

A backup options is to backup an entire database so that it can be restored to a previous point if necessary. Also, databases support version control of data, which means they actually store changes to each data element in any record so that if necessary only that particular field is restored.

1. **Electrical protection**
   1. **What is the role of a UPS?**

A UPS (or an uninterruptable power supply) can regulate electricity coming into a computer and supply backup electricity for a short time if a blackout occurs.

1. **Usernames & passwords**
   1. **What are the characteristics of a good password?**

Some characteristics of a good password is that they should have a mixture of upper and lower case characters, they should not be something that could be easily guessable (birthdays or names) and they should range between 7-15 characters.

* 1. **What is the role of access logs, audit trails and access restrictions?**

An **access log** is a list of all he requests for individual files that people have requested. An **audit trail** is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure or event. **Access restrictions** can control who can read or edit database objects. (*Information was gathered by the internet as I couldn’t find it in the textbook*).

1. **Systems security software**
   1. **What types of security software should organisations run?**

Some of the types of software that should be run by organisations include firewalls, antivirus types of data and software security software.

* 1. **Explain the nature of malware and phishing software**

Malware is malicious software which is specifically designed to disrupt or damage a computer system. Phishing is where hackers attempt to obtain sensitive and personal information (usernames, passwords, credit card details) by disguising themselves as a trustworthy entity in an electronic communication.

* 1. **Explain the nature of a firewall?**

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

1. **Encryption**
   1. **What does encryption involve?**

Encryption is the process of converting information or data into a code, which prevents unauthorised access.

* 1. **What protocols are used for encryption?**

Some protocols used for encryption are SSL, TLS and HTTPS

* 1. **What is hashing?**

Hashing is a method of encryption that can be used to encrypt the contents of databases inside fields; a method of protecting passwords by taking a variable-length password and creating a cryptic, fixed-length password from it by generating and using a salt value.